African Journal of Advanced Studies in Humanities and Social Sciences (AJASHSS)
المجلة الإفريقية للدراسات المتقدمة في العلوم الإنسانية والاجتماعية
Online-ISSN: 2957-5907
Volume 1,Issue 4,October-December 2022, Page No: 502-522
Website: https://aaasjournals.com/index.php/ajashss/index
Arab Impact factor 2022: 1.04 SJIFactor 2022: 4.338 ISI 2022: 0.510

أثر إدارة مخاطر التحول الرقمي في تحسين كفاءة أمن المعلومات "دراسة على المصارف التجارية الليبية"

أ. الصديق محمد خنفر[1]، د. حمزة محمد اكريم[2*]
[1]المدير العام لمصرف التجاري الوطني سابقاً، طالب دكتوراه، جامعة الجنان، لبنان
[2]عضو هيئة تدريس بكلية الاقتصاد، جامعة بنغازي، ليبيا

The impact of managing the risks of digital transformation in improving the efficiency of information security "Study on Libyan Commercial Banks"

Alsedig M. A. Khanfar[1 *], Dr. Hamza M Ekraim[2]
[1]Previous (CEO) and consultant Operation &amp, Financial at National Commercial Bank, Libya
[2]Department of Accounting, Faculty of Economics, University of Benghazi, Libya

[*]Corresponding author hamza.ekraim@uob.edu.ly [*]المؤلف المراسل
تاريخ النشر: 2022-12-21 **تاريخ القبول:** 2022-12-15 **تاريخ الاستلام:** 2022-11-22

الملخص
هدفت هذه الدراسة إلى معرفة أثر إدارة مخاطر التحول الرقمي في تحسين كفاءة أمن المعلومات في المصارف التجارية الليبية، حيث أن استخدام تكنولوجيا المعلومات والتحولات الرقمية المستمرة في القطاع المصرفي، أدي إلى وجود مسؤوليات جديدة فُرضت على المصارف بذل الجُهود لتفادي المخاطر الرقمية التي تنجم عن استخدامها، والتي قد تنشأ عن أخطاء محتملة تحدث خلال مراحل التعامل مع البيئة الرقمية، والتي تؤثر على أمن المعلومات، مما يؤدي الأمر إلى أضرار بمصالح مستخدمي المعلومات. اعتمدت الدراسة على المنهج الاستنباطي الاستقرائي وتم استخدام استمارة استبانة وتوزيعها على عينة شملت (145) مستجيباً من موظفي إدارة المخاطر والمحاسبة في المصارف الليبية والمراجعين بإدارة الرقابة والنقد بالمصرف المركزي، أستلم منها (126) استمارة صالحة للتحليل الإحصائي بنسبة (87%). توصلت الدراسة إلى وجود أثر ذو دلاله إحصائية لإدارة مخاطر التحول الرقمي المتمثلة بـ(إدارة مخاطر الداخلية والمرتبطة بالنظام الداخلي بالمصرف، إدارة مخاطر الخارجية والمرتبطة بعوامل خارج المصرف) في تحسين كفاءة أمن المعلومات في المصارف الليبية. وأوصت الدراسة بالتأكيد على المصارف التجارية الليبية زيادة الإهتمام بإدارة المخاطر الداخلية وحماية أمن المعلومات في ظل التحول الرقمي وتكنولوجيا المعلومات، لما تشكل أهمية أكبر مقارنة بالمخاطر الخارجية حسب نتائج الدراسة العملية، وغالباً ما تحدث المخاطر الخارجية بسبب ضعف رقابي داخل المؤسسة (مخاطر داخلية).

الكلمات المفتاحية: إدارة المخاطر، التحول الرقمي، أمن المعلومات.

Abstract

This study aimed to know the impact of digital conversion risk management in improving the efficiency of information security in Libyan commercial banks, whereas the use of information technology and continuous digital conversions in the banking sector led to the existence of new responsibilities that were imposed on banks to make efforts to avoid digital risks that result from its use, which may arise from potential errors that occur during the stages of dealing with the digital environment, and which affect the security of information security, which ultimately leads to damage the interests of users of information securty.

The study relied on the deductive and inductive approach, and a questionnaire was used and distributed to a sample that included (145) respondents from the directors of risk management and accounting in Libyan banks and auditors in the Central Bank's Control and Monetary Department,(126) valid forms received for statistical analysis at a rate of (87 %).

The study concluded that there is a statistically significant effect for managing the risks of digital conversion represented by (the internal risk management which associated with the internal system of the bank, the external risk management which associated with factors external the bank) in improving the efficiency of information security in Libyan banks. The study recommended emphasizing the Libyan commercial banks to pay attention to internal risk management and protect the information security in light of digital conversion and information technology, which forms great importance comparing to external risks according to the results of the practical study, external risks often occur with reasons related to inside the institution or a party to it (internal risks).

Keywords: Risk management, Digital transformation, Information security.

تمهيد:

أن جودة المعلومات تعتبر جزءَ لا ينفصل عن مسألة تطور المصارف واستقطاب المستثمرين، لذا فإن هناك مخاطر مترتبة على التحول الرقمي مما ينعكس على هذه المعلومات وكيفية تقيمها في المصارف. كما تساعد التكنولوجيا الرقمية في القطاع المصرفي في جمع كميات هائلة من البيانات وتخزينها، يمكن أن تكون هذه معلومات خاصة تتعلق بالعملاء أو المراسلين أو جهات ذات العلاقة، وربما يكون من الصعب جدًا الحفاظ على أمان هذه البيانات من مخاطر التحول الرقمي التي يجب أخذها في الاعتبار عند توجهنا صوب الرقمنة (خميس، 2021)، وهي كما هو مؤكد لا تعني التخلي عن التقنية الحديثة، وإنما استغلالها الاستغلال الأمثل ومحاولة تقليل مخاطرها وإدارتها بشكل أمثل. ويؤثر هذا التقدم التقني من تقنيات الذكاء الاصطناعي والحوسبة السحابية وإنترنت الأشياء وملياراتالأجهزة المتصلة بالإنترنت، بكونها أحد أهم ركائز الاقتصاد الرقمي الحديث، حيث عملت أزمة جائحة كورونا (covid-19) في تسريع وتيرة التحول الرقمي على مستويات عديدة (العنزي، 2020). ولكن هناك جانب آخر للاقتصاد الرقمي ونموه السريع يتصل بآثاره السلبية على البيئة، والفجوة الهائلة بين الدول الغنية والفقيرة التي تجعل مكاسبه مقتصرة على قطاعات وشركات ودول بعينها. وتقتضي معالجة هذه الآثار وتجنبها سياسات مرنة وتعاون على مستوى القطاعين العام والخاص(Muhrtala & Ogundeji 2013).

كما تُعد سياسات أمن المعلومات وتقيميها في القطاع المصرفي من الممارسات المهمة التي يعتمد عليها كثيراً في تنفيذ خطط المصارف التجارية في ظل التحول الرقمي وتحقيق أهدافه، حيث تربط بين أوجه العمليات المصرفية، والأهداف التي تسعى المصارف إلى تحقيقها عن طريق مهام وواجبات تقوم بها الإدارات العليا.

مشكلة الدراسة:

في وقت تتصاعد فيه وتيرة الهجمات الإلكترونية حول العالم، تجد المصارف نفسها في حاجة ماسة لمزيد من الإهتمام بإدارة التحول الرقمي في الفترة المقبلة، حيث بلغ حجم الخسائر التي تتكبدها المصارف الكبرى حول العالم بسبب الهجمات الإلكترونية بحسب تقرير حديث صادر عن (Risk IQ research) 25 دولارا في الدقيقة الواحدة، كما يتوقع حسب التقرير الصادر أن يشهد إنفاق المصارف على الأمن ضد الهجمات الإلكترونية والمخاطر الرقمية بالفترة المقبلة لنحو 170 مليار دولار وحتى 2022 مقارنة مع نحو 123 مليار دولار العام الماضي (Inaam, 2020). إن التطور الكبير الذي حصل في مجالات عدة، والتي من أهمها مجال تكنولوجيا المعلومات وأجهزة الحاسوب، أثر في علوم شتى، وذلك من أجل الاستفادة من الميزات التي توفرها هذه التكنولوجيا (Ismail & King, 2007).

هذا التطور أدى إلى استخدام أنظمة أمن المعلومات الإلكترونية في المصارف، وذلك لما توفره هذه الأنظمة من دقة في العمل، وسرعة في الإنجاز، وزيادة كفاءة أداء المحاسبين، والحصول على المعلومات المطلوبة بأسرع وقت، وبأقل تكلفة ممكنة، كما أدى إلى تعرض الأنظمة الإلكترونية إلى مخاطر عدة، تنعكس سلباً على صحة ومصداقية البيانات المتعلقة بتلك النظم (العنزي، 2020).

كما أن استخدام المصارف لتكنولوجيا المعلومات في ظل التحول الرقمي في البيئة المحلية، أدي لوجود مسؤوليات جديدة فُرضت عليها بذل المزيد من الجهود لتفادي المخاطر التي تنجم عن استخدام تلك التكنولوجيا، والتي قد تنشأ عن أخطاء محتملة تحدث خلال مراحل التعامل مع البيئة الرقمية، وذلك قد يؤثر على جودة المعلومات، وتؤدي لحدوث أضرار جسيمة على مصالحها، وكذلك على مصالح مستخدمي تلك المعلومات في اتخاذ القرارات (علي، 2011).

من هنا تكمن مشكلة الدراسة بهدف التعرف على أثر إدارة مخاطر التحول الرقمي الذي يشهده القطاع المصرفي في ليبيا في تحسين كفاءة أمن المعلومات.

أهداف الدراسة:

تهدف الدراسة بصفة أساسية إلى بيان أثر إدارة المخاطر في ظل التحول الرقمي والتطور التكنولوجي في تحسين كفاءة أمن المعلومات في المصارف الليبية، والذي يترتب عنها زيادة الثقة في تكنولوجيا المعلومات، وبالتبعية زيادة الثقة فيما تفرزه تلك النظم من معلومات وتقارير.

أهمية الدراسة:

تكتسب الدراسة أهمية خاصة من أن أساليب إدارة مخاطر التحول الرقمي سواء المخاطر الداخلية المرتبطة بالمؤسسة من الداخل أو المخاطر الخارجية المرتبطة بعوامل خارج المؤسسة في تحسين جودة وكفاءة المعلومات. كما أن سياسة أمن المعلومات المستخدمة حالياً في القطاع المصرفي في ليبيا لا تحد من مواجهة تعقيدات ذلك النوع من المخاطر (اكريم، 2021؛ شاكير، 2020؛ ديوان المحاسبة، 2020).

منهجية الدراسة:

تعتمد الدراسة على المنهج الاستنباطي الاستقرائي، وهو المنهج الذي مزج بين أسلوبي الاستنباط والاستقراء لدراسة تأثير إدارة مخاطر التحول الرقمي في تحسين كفاءة أمن المعلومات، وذلك من خلال الخطوات التالية:

• مراجعة الدراسات والأدبيات السابقة ذات العلاقة، للتعريف بأهمية إدارة مخاطر التحول الرقمي وأثرها علي أمن المعلومات بصفة عامة.

• تكوين نموذج الدراسة، ويتطلب ذلك بطبيعة الحال تحديد المتغيرات المختلفة الخاصة بإدارة مخاطر التحول الرقمي والتي يمكن أن تؤثر في تحسين كفاءة أمن المعلومات بصورة عامة كمتغير تابع.

• دراسة نموذج الدراسة في ضوء متغيرات البيئة المحلية للمصارف التجارية الليبية (مجتمع الدراسة) دراسة انتقاديه، وخبرة الباحثان في ضوء البيئة المحلية للتعرف على المتغيرات المختلفة الواردة بالإطار النظري العام للدراسة بصورة عامة والتي يمكن أن تؤثر في تحسين كفاءة أمن المعلومات بصورة خاصة.

الدراسات السابقة واشتقاق الفرضيات:

بينت دراسة **(سلايمي وبوشي، 2019)**، إلى التحول الرقمي بين الضرورة والمخاطر، حيث تناولت هذه الدراسة إلى أن التحول الرقمي يسهم في تأسيس اقتصاد رقمي يستطيع من خلاله الأفراد والشركات من رفع الطاقة الإنتاجية وخلق المكانة التجارية المحفزة والقادرة على المنافسة مما يزيد الشفافية على إدخال البيانات، ومن أهم النتائج التي توصلت إليها الدارسة أن التحول الرقمي يترتب عليه مخاطر متعددة ينبغي مواجهتها من خلال تطوير منظومات تواكب الثورة التكنولوجية والتطور التقني في تكنولوجيا وتعزيز أمن المعلومات الإلكترونية للحد من التلاعبات التي قد تحدث عليها.

أما دراسة **(أمين وآخرون، 2019)**، أوضحت الخطة المستقبلية التي يتطلع إليها نظم المعلومات في ظل تكنولوجيا الحوسبة السحابية، كما قدمت ملامح كل من أنظمة المعلومات والحوسبة السحابية، وأكدت أيضا على أن الحوسبة السحابية تعتبر واحدة من أحدث الاتجاهات في عالم تكنولوجيا المعلومات، وتقدم نموذجاً جديداً يقلل من تعقيد تكنولوجيا المعلومات من خلال توفير خدمات محوسبة عند الطلب في أي وقت وفي أي مكان عبر الإنترنت وفقا للبرمجيات ومعايير الأمن والسرية للبيانات.

أما دراسة **(العنزي، 2020)**، أوضحت مدى مساهمة التحول الرقمي في استخدام آليات ضبط مخاطر التكنولوجيا المالية لتطوير الخدمات المصرفية الإلكترونية بالمصارف الكويتية في ظل أزمة كوفيد 19، وتوصلت إلى أن تحليل وتصنيف المخاطر التكنولوجية المالية يساهم في تطوير الخدمات المصرفية في المصارف، كما أن التحول الرقمي في نظام الحوكمة يعطي نتائج واعدة ويحافظ على تكامل العمليات المصرفية الرقمية، وتوصى الدراسة إلى ضرورة إجراء دراسات تطبيقية على التكنولوجيا المالية بإعتبارها منطقة بحثية حديثة تمثل مجالاً خصبا للعديد من الدراسات المستقبلية التي يمكن أن تتناول أثر التكنولوجيا المالية على العديد من المتغيرات المختلفة.

كما تناولت دراسة **(Chinudzi, 2020)**، أثر الخدمات المصرفية الرقمية على الأداء المالي في المصارف التجارية زيمبابوي، واستخدم العائد على الأصول كمقياس للإداء المالي، واستخدمت الدراسة تحليل ارتباط لبيرسون وتحليل الانحدار، كما أثبتت الدراسة أن الخدمات المصرفية الرقمية ساهمت بشكل إيجابي في أداء المصارف التجارية في زيمبابوي من خلال زيادة ودائع العملاء عبر الإنترنت والمعاملات المصرفية، من ناحية أخرى، وتوصى الدراسة بأن تقدم المصارف التجارية في زيمبابوي خدمات عن طريق شبكات الهاتف المحمول المحلية الموثوق بها، لتقديم خدمات غير منقطعة وفعالة والتأكد أيضا من قيام شبكات الهاتف المحمول بتقديم خدمات مبتكرة مصممه خصيصاً لعملاء المصارف وقيام المصارف باستمرار بتحديث تقنيتها المصرفية الإلكترونية.

أما دراسة **(خميس، 2021)**، تطرقت إلى أثر التحول الرقمي على الأداء الوظيفي للعاملين في المصارف التجارية المصرية، وتوصلت هذه الدراسة إلى وجود تأثير إيجابي على التحول الرقمي والأداء الوظيفي، وذلك عن طريق المستوى العام لمجالات التحول الرقمي في المصارف التجارية المصرية وربطها بتجربة الموظف في مشاريع التحول، وتوصى الدراسة إلى ضرورة تطوير مهارات الموظفين في مجال الأتمتة وتقنية الروبوتات الذكية وتحليلات البيانات الضخمة، إضافة تحفيز الإبداع والابتكار.

ومن خلال عرض الدراسات السابقة وبيان أهمية التحول الرقمي وأثر على المعلومات والبيانات، فأن الدراسة تعتمد بيان أثر (إدارة مخاطر التحول الرقمي) كمتغير مستقل للدراسة، على تحسين (كفاءة أمن المعلومات) كمتغير تابع للدراسة.

ومن خلال الشكل التالي - رقم (1) - الذي يوضح نموذج الدراسة والذي تم تصميمة لتحديد العلاقة بين المتغير المستقل independent variable ووسائل قياسه المتمثلة في إدارة المخاطر الداخلية، وإدارة المخاطر الخارجية وأثرها على المتغير التابع dependent variable للدراسة المتمثل في (كفاءة أمن المعلومات)، **فأن الفرضية الرئيسية للدراسة هي:**

"إدارة مخاطر التحول الرقمي تؤثر تأثير جوهري في تحسين كفاءة أمن المعلومات "

ويتم قياسها من خلال الفرضيات الفرعية التالية:

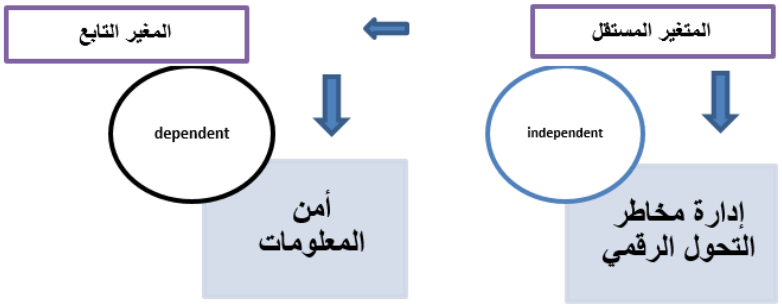
الفرضية الفرعية الأولى:

إدارة مخاطر التحول الرقمي الداخلية تؤثر تأثير جوهري في تحسين كفاءة أمن المعلومات "

الفرضية الفرعية الثانية:

إدارة المخاطر التحول الرقمي الخارجية تؤثر تأثير جوهري في تحسين كفاءة أمن المعلومات "

شكل (1) نموذج الدراسة Study model



وسائل القياس Means of measurement

إدارة مخاطر التحول الرقمي الداخلية	أمن المعلومات
إدارة مخاطر التحول الرقمي الخارجية	أمن المعلومات

المصدر: إعداد الباحثان بالاعتماد على استقراء الدراسات السابقة.

إدارة المخاطر وأمن المعلومات:

يعتبر مفهوم إدارة المخاطر أو إدارة المجازفة أو إدارة الخطر بالإنجليزية: **(Risk Management)** هي عملية قياس وتقييم للمخاطر وتطوير استراتيجيات لإدارتها، وتتضمن هذه الاستراتيجيات نقل

المخاطر إلى جهة أخرى وتجنبها وتقليل آثارها السلبية وقبول بعض أو كل تبعاتها **Kamala, 2021: (12)**. كما يمكن تعريفها بأنها النشاط الإداري الذي يهدف إلى التحكم بالمخاطر وتخفيضها إلى مستويات مقبولة. وبشكل أدق هي عملية تحديد وقياس والسيطرة وتخفيض المخاطر التي تواجه الشركة أو المؤسسة (كمال، 2021: 18).

وأوضحت دراسة **Inaam (2020)** إن إدارة المخاطر ما هي إلا ممارسة لعملية اختيار نظامية لطرق ذات تكلفة فعالة من أجل التقليل من أثر تهديد معين على المنظمة أو المؤسسة. والمخاطر لا يمكن تجنبها أو تقليص حدوثها بشكل كامل وذلك ببساطة يعود لوجود عوائق عملية ومالية، لذلك على كل المؤسسات أن تتقبل مستوى معين من الخسائر (مخاطر متبقية).

ومن جانب أخر فيما يخص إدارة المخاطر من حيث استخدام تكنولوجيا المعلومات والتحول الرقمي أوصت دراسة **(Nader, 2018)** أن هناك وجود مسؤوليات جديدة فُرضت على المؤسسات وقطاع الأعمال في بذل الجهود لتفادي المخاطر وإدارتها، والتي تنجم عن استخدام تلك التكنولوجيا، مما تنشأ أخطاء محتملة تحدث خلال مراحل التعامل مع البيئة الرقمية، وذلك قد يؤثر على أمن المعلومات، مما تسبب أضرار جسيمة على مصالح تلك المؤسسات، وكذلك على مصالح مستخدمي تلك المعلومات في اتخاذ القرارات المالية والإدارية.

وإن عملية التحول الرقمي يجب أن تمر بها جميع المؤسسات، وتحويل أعمالها وتطويرها للاستفادة من التقنيات وإدارة المخاطر التي تواجها، مثل الإنترنت هناك العديد من المخاطر الأمنية في التحول الرقمي الذي يجب مراعاتها (إنترنت الأشياء) والخدمات السحابية، وبالتالي فإن الإشارة إلى مخاطر التحول الرقمي لا تعني المطالبة بوقفه إذا كانت الرقمنة تُنذر بالخطر، فإن عدم التحول إليها يكون أكثر خطورة هذا التحول ليس خيارًا. (العرود وآخرون، 2011).

خاصة وأن الانتقال إلى الخِدْمَات الرقمية يوسع نطاق الهجوم بشكل كبير على البيانات، كما من الضروري أن تكون المؤسسات على دراية بمخاطر التحول الرقمي ولا تقلل من شأنها، فإن اتجاه إنترنت يعتبر هذا الشيء من كفاية الأعمال، ولكنه يضيف أيضًا مليارات الأجهزة غير الآمنة إلى الشبكة (Bodnar & William, 1995).

وبالتالي فإن أمان بيانات الأعمال والعملاء ذا أهمية قصوى، ولكن غالبًا ما يكون هناك خطر يتمثل في إمكانية التغاضي عن حماية هذه المعلومات وملكيتها عند تنفيذ أنظمة جديدة.

ومن جانب أمن المعلومات عرفها اكريم (2021:48) بأنها: "البحث في السياسات والاستراتيجيات التي ينبغي توخيها لحماية المعلومات التي تتعرض لها والمخاطر التي يمكن أن تهددها". وعرفها أيضا بأنها: "السياسات والإجراءات والمقاييس الفنية والتي تستخدم دون الوصول غير المعتمد أو السرقة أو التدمير السجلات".

وقام الباحثان **(Choga)** و **(Yose)** بتعريف أمن المعلومات بأنها " عبارة عن السياسات والممارسات والتقنية التي يجب أن تكون داخل المؤسسة لتداول حركات الاعمال عبر الشبكات بدرجة معقولة ومؤكدة من الأمان، هذا الأمان ينطبق على كل الأنشطة والحركات والتخزين الإلكتروني على شركات الأعمال والزبان والمنظمين والمؤمنين وأي شخص أخر ممكن أن يكون معرضا لمخاطر الاختراق"

(Yose & Choga, 2016:28).

كما أن استراتيجية أمن المعلومات أو سياستها في ظل التحول الرقمي هي "تلك القواعد التي يطبقها الأشخاص لدي التعامل من التقنية ومع المعلومات داخل المنشأة وتتصل بشؤون الدخول الي المعلومات والعمل على نظمها وإدارتها" (العنزي، 2020 :37).

حيث تعد استراتيجية أمن المعلومات مهمة جدا للحفاظ على أمن المعلومات بحيث تمنع الأشخاص الذين لا يحق لهم الوصول الي المعلومات أن يصلو الي تلك المعلومات أو التعامل معها أو التعرف عليها.

ومن أجل حماية المعلومات من المخاطر التي تتعرض لها المؤسسات والشركات في ظل التحول الرقمي لابد من توفر مجموعة من العناصر التي يجب أخذها بعين الاعتبار لتوفير الحماية الكافية للمعلومات، ولقد صنفت تلك العناصر الي خمسة عناصر وهي (جمعة، 2003):

• **السرية أو الموثوقية:** وهي تعني التأكد من أن المعلومات لا يمكن الاطلاع عليها أو كشفها من قبل أشخاص غير مصرح لهم بذلك ولتجسيد هذا الامر يجب على المؤسسة استخدام طرق الحماية المناسبة من خلال وسائل عديدة مثل عمليات تشفير الرسائل أو منع التعرف على حجم تلك المعلومات أو مسار إرسالها.

• **التعرف أو التحقق من هوية الشخصية:** وهذا يعني التأكد من هوية الشخص الذي يحاول استخدام المعلومات الموجودة ومعرفة ما إذا كان هو المستخدم الصحيح لتلك المعلومات أم لا، ويتم ذلك من خلال استخدام كلمات السر الخاصة بكل مستخدم، وتوضح مؤسسة **(RSA)** لأمن المعلومات **RSA Security Inc** ثلاث طرق للتحقق من الشخصية وهي: الاولي: عن طريق شيء يعرفه الشخص مثل كلمة المرور، والثانية: عن طريق شيء يملكه مثل رسالة التشفير **(Token)** وهي عبارة عن كود يقوم بدخالة المستخدم للحاسوب للحيازة على صلاحية التشغيل أو الشهادة الالكترونية، والثالثة: عن طريق شيء يتصف به الشخص من الصفات الفيزيائية مثل بصمة الاصبع او المسح الشبكي أو نبرة الصوت، وكل طريقة لها إيجابيات وسلبيات، وتنصح مؤسسة **(RSA)** باستخدام طريقتين مع بعضهما البعض من هذه الطرق الثلاثة.

• **سلامة المحتوي:** وهي تعني التأكد من أن محتوي المعلومات صحيح ولم يتم تعديله أو تدميره أو العبث به، في أي مرحلة من مراحل المعالجة أو التبادل سواء كان التعامل داخليا أو خارجيا من قبل أشخاص غير مصرح لهم بذلك ويتم غالبا بسبب الاختراقات الغير مشروعة مثل الفيروسات حيث لا يمكن لأحد أن يكسر قاعدة بيانات المصرف ويقوم بتغيير الرقم او رصيد حسابة، لذلك يقع على عاتق المؤسسة تأمين سلامة المحتوي من خلال إتباع وسائل حماية مناسبة مثل البرمجيات والتجهيزيات المضادة للاختراقات أو الفيروسات.

• **استمرارية توفير المعلومات أو الخدمة:** وتعني التأكد من استمراريه عمل نظام المعلومات بكل مكوناته واستمرار القدرة على التفاعل مع المعلومات وتقديم الخدمات لمواقع المعلومات وضمان عدم تعرض مستخدمي تلك المعلومات إلى منع استخدامها أو الوصول إليها بطرق غير مشروعة ويقوم بها أشخاص لإيقاف الخدمة.

• **عدم الإنكار:** ويقصد به ضمان عدم إنكار الشخص الذي قام بإجراء معين متصل بالمعلومات لهذا الإجراء، ولذلك لابد من توفر طريقة أو وسيلة لإثبات أي تصرف يقوم به أي شخص للشخص الذي قام به في وقت معين، ومثال على ذلك للتأكد من وصول بضاعة تم شراؤها عبر شبكة الانترنت الي صاحبها، ولإثبات تحويل المبالغ إلكترونيا يتم استخدام عدة رسائل مثل التوقيع الإلكتروني والمصادقة الإلكترونية.

تعتبر مسألة حماية أمن المعلومات أمن المسائل الهامة والضرورية والتي ينبغي على المؤسسة أخذها بعين الاعتبار، ووضع خطة شاملة في حدود امكانياتها التنظيمية والمادية ويجب أن تكون تلك الحماية قوية وليست ضعيفة ولذلك فإنه توجد عدة متطلبات لحماية أمن نظم المعلومات تتمثل في **Nader, (2018) :**

• وضع سياسة حماية عامة لأمن نظم المعلومات تتحدد حسب طبيعة عمل وتطبيقات المنظمة أو الشركة.
• يجب على الإدارة العليا في الشركة دعم أمن نظم المعلومات لديها.
• يجب أن توكل مسؤولية أمن نظم المعلومات في الشركة لأشخاص محددين، وتحديد اختصاصات وصلاحيات الرقابة والتفتيش لنظم المعلومات والشبكات الحاسوبية.

• الاحتفاظ بنسخ احتياطي لنظم المعلومات بشكل أمن، وتشفير المعلومات التي يتم حفظها وتخزينها ونقلها على مختلف الوسائط.
• تأمين استمرارية عمل وجاهزية نظم المعلومات، خاصة في حالة الازمات ومواجهة المخاطر المتعلقة بالنظم.
وكذلك فأن تطور تكنولوجيا المعلومات ومع الانتشار الواسع لتطبيق النظم المعلومات بطرق إلكترونية واختفاء العمل على النظم اليدوية أو شبه انعدم، أصبحت هناك حاجة ماسة لحمايتها من المخاطر التي تتعرض لها، فأن الرقابة على نظم المعلومات تقسم الي ثلاث مجموعات رئيسية **Yose & Choga, (2016)** حسب مراحل النظام وهي:
أولا: الرقابة على المدخلات: وهي تهدف إلى التأكد من أن البيانات تم إدخالها الي النظام أدخلت في الوقت المناسب وبشكل صحيح، وضمان سير تلك البيانات خلال خطوط الاتصال وعدم فقدها أو تغييرها واكتشاف أي أخطاء تتعلق بالبيانات قبل عملية تشغيلها وذلك لضمان خلو البيانات المدخلة من أي أخطاء وليتم الحصول على مخرجات سليمة بناء على مدخلات سليمة ولذلك فلا بد من الحصول على مدخلات البيانات في مرحلة مبكرة من مراحل معالجتها في النظام، وذلك لأسباب التي اشارت اليها دراسة **Al Hanini** (2012):
• إمكانية تصحيح الأخطاء التي تم اكتشافها في البيانات التي تم رفضها في بداية ادخلها والرجوع الي المستندات الخاصة بها وفحص أسباب رفضها.
• ان البيانات التي تم إدخالها بشكل صحيح ليس من الضروري ان تكون بيانات جيدة ولذلك يجب اجراء اختبارات أخري لفحصها خلال مراحل تداولها ومعالجتها.
• خلو نظام المعلومات من بيانات غير دقيقة في المراحل الأخيرة لعمليات المعالجة يمكن من حماية ووقاية الملفات الرئيسية وعمليات المعالجة في خطواتها الأخيرة.
• اعتماد نظام المعلومات على مدخلات جيدة يمكنه من الحصول على مخرجات جيدة.
ثانيا: الرقابة على التشغيل: وهي التحقق من أن تشغيل البيانات تم بصورة دقيقة وبشكل صحيح وأنه تم معالجة كافة العمليات المتعلقة بالتشغيل وقد تم استخدام جميع البرامج المناسبة واللازمة لعملية التشغيل ومن أهم الوسائل الرقابية على تشغيل البيانات ما يلي **:(Nader, 2018)**
• تطبيق الاختبارات التي تتضمن صحة عمليات التشغيل بحيث يتم رفض التعامل مع المدخلات أو المخرجات غير الصحيحة.
• استكمال مسار المراجعة الذي يمكن من تتبع سجل عملية من عمليات التشغيل، والمساعدة في اعداد القوائم المالية.
• تزويد برامج التشغيل بوظائف ومهام تمكن من تسجيل أي عملية محاولة للتدخل في عمل البرنامج أثناء عملية التشغيل والمعالجة.
ثالثا: الرقابة على المخرجات: وهي تهدف للتأكد من أن نتائج مخرجات عملية التشغيل كاملة وصحيحة وجيدة ودقيقة، وانه تم تسليمها وتوزيعها للأشخاص المسموح لهم باستلامها والاطلاع عليها، وتستند الرقابة على المخرجات على الرقابة السابقة وهي عملية الرقابة على تشغيل البيانات، فإذا كانت الرقابة على المدخلات وعلى عملية التشغيل جيدة ودقيقة هذا يؤدي الي الحصول على مخرجات سليمة ودقيقة.
حيث أشارت دراسة **(Yose & Choga, 2016)** أن متطلبات الرقابة لنظم المعلومات تنتهج عدد من الإجراءات الحماية، منها :
• إجراءات الحماية الفزيائية لأمن المعلومات بما فيها الحماية المادية للأجهزة والتي تحتوي على النظم المعلومات.

• إنتقاء العاملين في النظم المعلوماتية بحيث يكونوا ذوي خبرة وثقة وأمانه ويعملون لمصلحة المؤسسة وتوعيتهم أمنيا للمحافظة على أمن المعلومات.
• إجراءات الحماية الخاصة بالشبكات المعلوماتية ومنع اختراقها.
• العمل على تشفير المعلومات التي يتم تخزينها ونقلها حتى لا يتم معرفة ماهيتها في الحصول عليها من أشخاص غير مصرح لهم بذلك.
• إجراءات حفظ البيانات بصورة عامة إلكترونية منها والمستندية، وحفظ نسخ منها في أمكان أمنه يمكن الرجوع اليها.
• إجراءات ضمان استمرارية عمل وجاهزية المعلومات في شتي الظروف التي قد تواجه المؤسسة، مثل التعطل أو توقف النظم المعلوماتية.

تعتبر حماية البيانات والمعلومات من الأمور الواجب الاهتمام بها في كافة مراحل إعداد نظم المعلومات حيث أن أمن المعلومات والبيانات أصبح من أهم عناصر الرقابة الواجب تطبيقها على المعلومات من خلال التخطيط المستمر خلال دورة حياة نظم المعلومات المستخدمة (Yorozu et al, 1982).

وتكمن خطورة مشاكل أمن المعلومات في عدة جوانب منها تقليل أداء الأنظمة الحاسوبية، أو تخريبها بالكامل مما يؤدي الي تعطيل الخدمات الحيوية للمؤسسة، اما الجانب الأخر فيشمل سرية وتكامل المعلومات حيث قد يؤدي الي الاطلاع والتصنت على المعلومات السرية أو تغييرها الي خسائر مادية أو معنوية كبيرة.

تحدث مخاطر المعلومات بالشركات سواء اهتمت إدارة الشركة باكتشاف تلك المخاطر وإدراكها بالفعل أو لم توليها العناية الكافية، ويؤدي تعقد تكنولوجيا المعلومات إلى صعوبة تفهم مخاطر المعلومات ، وبالتبعية صعوبة اتخاذ القرارات الجيدة بشأنها، ومن ناحية أخري تتأثر المعلومات بالبيئة المحيطة شأنه في ذلك شأن أي نظام للمعلومات. وقد صاحب التطورات السريعة والمتلاحقة في مجال تكنولوجيا المعلومات والاتصالات العديد من المخاطر البيئية التي تؤثر على نظام المعلومات وعلى القوائم المالية للشركة، وتتمثل تلك المخاطر فيما يلي (العنزي، 2020):

- **الاحتيال:** يعرف الاحتيال في هذه الحالة بأنه عمل غير قانوني يستخدم في ارتكابه معلومات الحاسوب وتكنولوجيا المعلومات، ويرتبط الاحتيال في هذه الحالة بالعنصر البشري، حيث لا يتم الاحتيال من خلال نظام الكمبيوتر بدون تدخل الانسان
- **الخطأ:** تتسم الخسائر المتعلقة بالأخطاء بأنها متنوعة إلى حد كبير، ويعتمد ذلك بصفة أساسية على المكان الذي حدث فيه الخطأ، والوقت المستغرق في تحديد الخطأ وتصحيحه. ولا جدال أن تنفيذ الرقابة المانعة التي تكتشف وتتصحح الأخطاء قبل أن تحدث، يمكن أن تمنع الخسائر المالية المترتبة على الأخطاء والتأثير السلبي لها على أهداف المنظمة(Muhrtala & Ogundeji 2013).
- **قطع الخدمة أو تأخيرها:** قد يترتب على تأخير عملية تشغيل المعلومات أو قطع الخدمة أن تتوقف الاعمال بالمنظمة، حيث أن ذلك التأخير من شأنه أن يؤدي الي عدم إنجاز مهام المقبوضات والمدفوعات في الوقت المناسب، وتنشأ مخاطر قطع الخدمة نتيجة أسباب عرضية أو تجاهل بعض المسببات مثل إنتهاء صلاحية برنامج مقاومة الفيروس أو بسبب شخص يتعمد.
- **الإفصاح عن معلومات سرية:** ويشير هذا النوع من المخاطر إلى الكشف عن معلومات لها طبيعتها السرية، مثل تلك الخاصة بالعملاء، وغني عن البيان حرص إدراه المنظمة علي سرية البيانات الخاصة بعملائها وموظفيها هو السبيل لمكافحة هذا النوع من المخاطر.
- **الإختراق:** وينطوي هذا النوع من المخاطر على إمكانية الوصول الي النظام عن طريق إقتحام الإجراءات الأمنية للنظام أو عن طريق استغلال نقاط الضعف في نظم الرقابة.

ويهدف القائم بالاختراق إلى تحقيق ربح من وراء هذا الاختراق، أو قد يكون لغرض التسلية او غير ذلك، فإذا كان الهدف هو تحقيق أرباح فان المخترق سيسعى إلى اختراق نظم الخاصة بالمنظمات محددة ولمعلومات محددة، أما إذا كان الهدف مجرد التسلية فإن الاقتحام يتم لنظم وبيانات يسهل الوصول إليها ولا يتوفر لها وسائل الحماية الكافية (IAASB, 2021).

- **سرقة المعلومات:** وتتعلق تلك المخاطر بسرقة البيانات والمعلومات ذات القيمة الخاصة بالمنظمة، ومن امثلتها خطط التسوق والحملات الاعلانية واسرار المهنة وبيانات البحوث والتطوير للمنتجات الجديدة وقوائم العملاء، ومن شأن هذا النوع من السرقات للبيانات والمعلومات أن يؤدي الي خسائر كبيرة للمنظمات.

- **التلاعب بالمعلومات:** يحدد التلاعب بالمعلومات في أي مرحلة من مراحل تشغيل المعلومات، بداية من مرحلة المدخلات وحتى مرحلة المخرجات.

ويعد التلاعب في مرحلة المدخلات هو الأكثر شيوعاً نظرا لسهولة إنجازه كما يصعب اكتشافه، ولا يتطلب مهارات عالية في النظم لاختراقها، ويتأسس التلاعب في البرامج على إحداث تعديل أو إدخال عمليات محددة في نظام المعلومات، وكما يعد التلاعب مهمة صعب إنجازها ويصعب اكتشافها، ويتطلب اكتشافها وتعديها مهارات عالية في البرمجة.

- **مخاطر برامج الفيروسات:** يصيب الفيروس النظام ويعدل في بياناته.

- **هجمات إعادة الخدمة:** يؤدي هذا النوع من المخاطر إلى عرقلة نظم الكمبيوتر وشبكات المعلومات عن أداء مهامها طبقا للغرض المحدد من آجلة، وتسبب تلك الهجمات قصور في الخدمة بالنسبة للمستخدم عن طريق استنفاد الموارد النادرة مثل كمية البيانات والذاكرة، ويمكن أن تعطل العناصر المادية.

- **تشويه (إفساد) مواقع على شبكة الانترنت**: ويتم في هذا النوع من المخاطر إجراء تعديلات على الموقع الالكتروني على شبكة الانترنت بهدف توصيل رسالة ما، أو السخرية من المنظمة، أو ترك علامة ما على الموقع (Muhrtala & Ogundeji 2013).

- **الابتزاز**: يأتي هذا النوع من المخاطر نتيجة لنجاح أحد الأشخاص في سرقة معلومات من أحد المنظمات، أو قدرته على إعاقة نظم المعلومات بالمنظمة وتعطيلها، ويصبح مرتكب تلك الجريمة بهذا الشكل في موقع يمكنه من تهديد المنظمة بكشف تلك المعلومات التي في حوزته أو تعطيل النظام بها في حالة عدم تحقيق مطالبه.

وقد صنفت جمعية مراجعة ومراقبة نظم المعلومات **The Information Systems Audit and Control Association (ISACA)** مخاطر نظم المعلومات إلى أربع مجموعات أساسية: مخاطر بشرية (الادخال)، ومخاطر برامج والتكنولوجيا معلومات (الاختراقات والفيروسات الحاسوب)، مخاطر المنافسة أو السوق (نظم ومعلومات)، مخاطر بيئية (الكوارث الطبيعية).

- **ضعف وقصور في أحد أو بعض نظم الرقابة:** وينشأ ذلك بصفة أساسية عند اختيار نظم رقابة غير ملائمة.
- **التواطؤ:** قد يكون تواطؤ بين أثنين أو أكثر من العاملين داخل المنظمة بغرض الاحتيال، كما قد يكون بين أحد العاملين أخر من خارج المنظمة وأيضا بغرض الاحتيال.
- **ضعف التنفيذ:** فقد تتبني المنظمة سياسات إدارية ونظم رقابية ملائمة الا انه لا يتم الالتزام بها أو مخالفتها عند التنفيذ.
- **جرائم الكمبيوتر:** وفي هذا النوع من الجرائم يستخدم الكمبيوتر سواء بطريقة مباشرة أو بطريقة غير مباشرة، ويعد التخريب في الكمبيوتر ومحتوياته من

جرائم الكمبيوتر المباشرة، أما الوصول غير المسموح به فأنه يعد من جرائم الكمبيوتر غير المباشرة. ويتأثر درجة ومستوي تعرض نظام المعلومات للمخاطر بالعوامل التالية (خميس، 2020):

• **التكرار:** كلما زاد تكرار حدوث الحدث كلما زادت درجة تعرضه للمخاطر.
• **الحساسية (وجود ثغرة):** كلما زادت نقاط الضعف في الأصول أو كلما كانت أكثر حساسية كلما كانت أكثر عرضة للمخاطر.
• **الحجم:** كلما زادت القيمة النقدية للخسارة المحتملة كلما زادت درجة التعرض للمخاطر.
كما أن مخاطر المعلومات قد يكون لها أثارا مالية أو أثاراً على السمعة أو أثاراً قانونية أو أثارا على العملاء، أو المنافسة وبصفة عامة تؤثر المخاطر على نظم المعلومات في أربعة جوانب أساسية (Muhrtala & Ogundeji 2013):
• **الإتاحية:** وهي تشير الي احتفاظ نظام المعلومات بالعمليات الحالية بالترتيب، ومرتبة باستمرار، وايضاً حمايتها من التوقف.
• **إمكانية وسهولة الوصول الي المعلومات**: والتي تتضمن سهولة وصول الافراد للمعلومات التي يحتاجونها، الا أن تلك الميزة لا يجب أن تتوفر للأفراد غير المصرح لهم بالوصول للنظام.
• **الدقة**: يقدم النظام المعلومات الكاملة التي تواجه متطلبات الإدارة والعملاء والموردين، في التوقيت المناسب، وبمستوي الدقة المطلوبة.
• **القدرة على تنفيذ التغيرات الاستراتيجية الأساسية:** قدرة نظم المعلومات على المشاركة في تنفيذ استراتيجية جديدة، مثل الاستحواذ على شركة أو اكتمال إعادة تصميم عملية جديدة أو الترويج لسلعة أو خدمة في السوق (Muhrtala & Ogundeji 2013).
كما أن المعلومات وبالأخص بعد التطورات المتلاحقة في الأنظمة المحاسبية وانتقالها من العمل اليدي الي العمل الالكتروني، اصبحت أكثر مخاطرة واقل اماناً من الأنظمة التقليدية (اليدوية)، ونظراً لاعتماد أنظمة المعلومات المحاسبية حالياً علي البيئة الالكترونية (تكنولوجيا المعلومات)، وحفظ بياناتها علي ملفات الكترونية يستطيع عدد كبير من الأشخاص الوصول إليها، ولذلك تتعرض نظم المعلومات للعديد من المخاطر التي تهدد امنها وذلك بسبب مجموعة من العوامل والتي يذكرها (Ismail & King, 2007) منها: الكم هائل من البيانات ولذلك فانة يصعب عمل نسخ ورقية لها، وصعوبة اكتشاف الأخطاء، وصعوبة مراجعة الإجراءات، وصعوبة تغيير النظم الالية مقارنة بالنظم اليدوية، و احتمال تعرض النظم الآلية إلي إساءة استخدامها بواسطة الخبراء غير المنتمين للمنظمة في حال استدعائهم لتطوير النظم.

مخاطر التحول الرقمي وأمن المعلومات في المصارف الليبية:

يعاني أمن المعلومات في القطاع المصرفي في ليبيا العديد من المخاطر التي تهدد أمنها، حيث أن المصارف تعمل على النظم الآلية والتي تعتمد على تكنولوجيا المعلومات والتي تواجهه أخطاء بشكل متكرر سواء كانت مخاطر غير متعمدة أو متعمدة، وكذلك عملية تبادل الأرقام المخولة بالاستخدام بين الموظفين وبشكل مستمر (ديوان المحاسبة الليبي، 2020).
كما أشارت العديد من الدراسات أن القطاع المصرفي في ليبيا يعاني العديد من المخاطر الرقابية على أنظمة معلوماتها، وتعرض المصارف الليبية للعديد من الخسائر بسبب عدم إيجاد وسائل مناسبة للحد من مخاطر العمل المصرفي (اكريم، 2021؛ شاكير، 2020).
وأشارت تقارير ديون المحاسبة للسنوات (2017-2020) تراكم القضايا المرفوعة ضد القطاع المصرفي في ليبيا، وبمبلغ كبيرة حتى نهاية عام 2020، بمبلغ يفوق 22,150,700 ديناراً ومبلغ 12,094,639 دولار امريكي لعدد 356 قضية، والبيان التالي يوضح القضايا التي لها علاقة مخاطر أمن المعلومات كما هو مبين بالجدول رقم (1).

كما توصلت دراسة (شاكير، 2020) لعدد من النتائج المتعلقة بالأنظمة المحاسبية في المصارف التجارية الليبية، أن تلك النظم الموجودة حالياً بالقطاع المصـــرفي لم تقم بتحديد تكلفة الخدمات التي تقدمها للعملاء بشـكل أمثل، وعدم إمكانية إسـتخدام وإعداد الميزانيات التقديرية في القطاع المصـرفي من خلال أنظمة المعلومات المستخدمة حالياً بشكل أمثل.

كما أن أمن المعلومات القائم بالقطاع المصـرفي حالياً يعاني من قصـور شـديد فيما يخص ضـعف أداء العاملين في القطاع المصرفي، من خلال عدم حصولهم على التدريب الكافي على المنظومات المصرفية، وضـعف المسـتويات التعليمية للمراجعين الداخلين، وعدم درايتهم بأسـس المراجعة الالكترونية ومعايير المراجعة الداخلية بالقطاع المصرفي (أكريم، 2021).

كما توصلت دراسة (شاكير، 2020) بأن المصارف التجارية العامة والتي تعتبر هي المهيمن على السوق المصـــرفي في ليبيا تعاني من ضـــعف في الأداء الرقابي ومواجهة المخاطر التي تصـــيب عمل الأنظمة المحاسبية بها، ومن أهم نتائج الدراسة ان المخاطر التشغيلية كلفت المصارف العديد من الخسائر وتأكل في الأموال وان أي كوراث أو مخاطر بيئية لن يجد المصـــرف أي وســـائل حماية مناســـبة لها، طبقا للإجراءات الحالية المتبعة بالقطاع المصرفي في ليبيا.

جدول (1): القيمة التقديرية للقضاياً المرفوعة ضد المصارف التجارية مخاطر أمن المعلومات.

م	القضايا المرفوعة ضد المصرف	القيمة بالدينار	القيمة بالدولار	عدد القضاياً			
				مصرف الجمهورية	مصرف الوحدة	مصرف الصحاري	مصرف شمال أفريقيا
1	التلاعب في الحسابات	1,150,400	**$ 310,141**	3	1	1	-
2	حسابات المقاصة	1,256,450	**$ 322,167**	7	3	-	1
3	تزوير صكوك	1,850,960	**$ 474,605**	4	-	5	2
4	تلاعب بيانات العملاء	1,000,000	**$ 256,410**	5	2	1	-
5	الاعتمادات المستندية	5,982,163	**$1,533,888**	4	2	3	1
6	تزوير مستندات	1,563,455	**$ 400,886**	2	-	1	-
7	أفشاء أسرار العملاء	500,000	**$ 128,205**	2	-	-	-
8	اختلاسات من الحسابات	3,652,320	**$ 936,492**	5	2	3	3
الإجمالي		16,955,748	$4,862,794	**32**	**10**	**14**	**7**

المصدر: (اكريم، 2021: 146)

الدراسة الميدانية:

مجتمع وعينة الدراســة: يتمثل مجتمع الدراســة في المجموعة من الصــفات الوظيفية والتي لها علاقة بموضــوع الدراســة وأهدافها، والمتمثلة في الموظفين بإدارة المخاطر والمعلومات والبيانات بالقطاع المصـرفي في ليبيا، وقد تم توزيع عدد (145) استمارة استبيان على مجتمع وعينة الدراسة، أُستلم منها عدد (126) استمارة استبيان صالحة للتحليل الإحصائي، وبلغت نسبة الردود (87%)، كما هو موضح في الجدول (2).

جدول (2) نسبة الردود

مسلسل	البيان	المجتمع	العينة	الاستمارات المستلمة		الفاقد	
				العدد	النسبة	العدد	النسبة
1	إدارات المالية والمحاسبة بالمصارف التجارية	115	86	77	90%	9	10%
2	إدارات المخاطر بالمصارف التجارية	54	37	31	84%	6	16%
3	إدارة الرقابة على المصارف والنقد ب م ل م	36	22	18	82%	4	18%
	الإجمالي	205	145	126	87%	19	13%

- **تحليل الثبات (Reliability Analysis):** تم التأكد من ثبات أسئلة استمارة الاستبيان، من خلال اختبار معامل آلفا كرونباخ لمجتمع وعينة الدراسة والتي تمثلت في ثلاث مجموعات، ولقد قام الباحثون بتوزيع الاستمارات عليهم، وبعد تجميع هذه الاستمارات تم إجراء اختبار آلفا كرونباخ على جميع أسئلة استمارة الاستبيان المتعلقة بالجزء الثاني وعددها (12) سؤال وجد أنه يبلغ 96.3%، وتدل هذه القيمة على أن للاستبيان درجة ثبات مقبولة إحصائياً تدعو إلى الثقة.

جدول (3) تحليل الثبات

المحور	عدد الفقرات	معامل Cronbach's alpha
إدارة المخاطر الداخلية للتحول الرقمي	5	0.891
إدارة المخاطر الخارجية للتحول الرقمي	7	0.751
المعامل الكلي	**12**	**0.963**

كما أظهرت أيضاً نتائج التحليل الإحصائي للبيانات الديمغرافية للمشاركين في الدراسة أن التأهيل العلمي للمشاركين ترتكز بين تعليم جامعي (بكالوريوس) وعالي (ماجستير ودكتوراه) تجاوزت نسبته 80% من العدد الكلي، وأن الخبرة المهنية تتجاوز 10 سنوات لأكثر من 59% من المشاركين الدراسة، وهذا يعطي مؤشر جيد للاعتماد على إجابات المشاركين بالدراسة كما هو موضح بالجدول رقم (4).

جدول (4) التأهيل العلمي والخبرة المهنية

المجموعة	العدد	المؤهل العلمي				عدد سنوات الخبرة			
		دكتوراه	ماجستير	بكالوريوس	أخرى	اقل من 5	من 5 اقل من10	من 10 اقل 20	أكثر من 20
إدارات المالية والمحاسبة بالمصارف التجارية	77	9	25	41	2	0	35	24	18
%	100%	12%	32%	53%	3%	0%	45%	31%	23%
إدارات المخاطر بالمصارف التجارية	31	2	3	25	1	0	11	18	2
%	100%	6%	10%	81%	3%	0%	35%	58%	6%
إدارة الرقابة على المصارف والنقد ب م ل م	18	1	5	7	5	0	5	9	4
%	100	6%	28%	39%	28%	0%	28%	50%	22%
الإجمالي	126	12	33	73	8	0	51	51	24
%	100	10%	26%	58%	6%	0%	40%	40%	19%

التحليل الإحصائي لإدارة المخاطر التحول الرقمي:

أولا: الإحصـــاء الوصـــفي – إدارة المخاطر الداخلية للتحول الرقمي: تبين نتائج التحليلات الإحصـــائية الواردة بالجدول (5) أن المتوسط الحسابي الإجمالي للنتائج الإحصائية:

جدول (5) الاحصاء الوصفي – إدارة مخاطر التحول الرقمي الداخلية

ر.م	الفقـرات	Mean	dev- Std	Min Max	الموافقة ورفض	قوة تأثير
1	إجراءات إدارة المخـاطر – العـاملين والمســؤولين بـالمؤســســة – جوانـب الرقـابيـة للهيكـل التنظيمي بالمصرف – الصلاحيات – المسؤوليات – والإجراءات التنظيمية.	4.425	0.875	Max	موافقة بشدة	تأثير قوي جداً
2	إجراءات إدارة المخـاطر – العـاملين والمســؤولين بالمؤسسـة – المتعلقة بالميثاق شـرف المهنة وأخلاقيات العمل والسمعة – عند التعيين – عند العمل.	4.521	0.759	Max	موافقة بشدة	تأثير قوي جداً
3	إجراءات إدارة المخـاطر التقنيـة – حمـايـة الأجهزة والأرقام السرية وتدويرها – كاميرات المراقبة – برامج الحماية – المراجعة الالكترونية.	4.266	0.999	Max	موافقة بشدة	تأثير قوي جداً
4	إجراءات حوكمة تكنولوجيا المعلومات وتفعيل أساسيات الحوكمة الإلكترونية وسياسة أمن المعلومات والشبكات.	4.208	1.012	Max	موافقة بشدة	تأثير قوي جداً
5	إجراءات الخاصـــة بالتعاقد مع شـركات الدولية لحماية الاختراقات من داخل المؤسسة والوصول غير المصرح به للبيانات وتعديلها.	3.756	0.768	Max	موافقة	مؤثر
	التحليل الاحصائي الكلي للمتغيرات	4.235	0.882	Max	موافقة بشدة	تأثير قوي جداً

حيث يتراوح بين (4.521) للسـؤال: " إجراءات إدارة المخاطر – العاملين والمسـؤولين بالمؤسـسـة – المتعلقة بالميثاق شـــرف المهنة وأخلاقيات العمل والســـمعة – عند التعيين – عند العمل"، مما يعني أن الاتجاه العام لإجابات المشـاركين يوافقون بشـدة على الأسـئلة، و (3.756) للسـؤال: " إجراءات الخاصـة بالتعاقد مع شـركات الدولية لحماية الاختراقات من داخل المؤسـسـة والوصـول غير المصـرح به للبيانات وتعديلها " تبين أنهم يوافقون على أثر إدارة المخاطر الداخلية للتحول الرقمي.

ثانيا: الإحصاء الاستدلالي (الاستنتاجي) لإدارة المخاطر الداخلية للتحول الرقمي:

تم أجراء اختبار تحليل التباين الأحادي (One- Way ANOVA) واختبار و-One Way Kruskal Wallis من خلال عرض قيم كل ســؤال على حده كما هو موضـــح بالجدول (6)، بينت النتائج أن قيمة (P- Value) أكبر من مسـتوى الدلالة المعنوية 5% في اغلب الأسـئلة، مما يعني عدم وجود فروق ذات دلالة إحصـائية فيما بين متوسطات المجموعات لكل سؤال من هذه الأسئلة، اما باقي الأسئلة بينت النتائج أن قيمة (P- Value)أقل من مستوى الدلالة المعنوية 5%، كما هو موضح بالجدول رقم (6) الاختلافات بين اجابات الشركات بسبب متغير (الخبرة) والتأهيل العلمي للمشاركين.

جدول (6) - الاحصاء الاستنتاجي – إدارة مخاطر التحول الرقمي الداخلية

ر.م	الفقــرات	One–Way Anova	One-Way K.W	MCT
1	حماية المعلومات– العاملين والمسؤولين بالمؤسسة – جوانب الرقابية للهيكل التنظيمي بالمصرف – الصلاحيات – المسؤوليات – والإجراءات التنظيمية.	0.348	0.208	لا توجد إختلافات جوهرية
2	حماية المعلومات– العاملين والمسؤولين بالمؤسسة – المتعلقة بالميثاق شرف المهنة وأخلاقيات العمل والسمعة – عند التعيين – عند العمل.	0.471	0.014	توجد إختلافات جوهرية
3	حماية المعلومات– حماية الأجهزة والأرقام السرية وتدويرها – كاميرات المراقبة – برامج الحماية – المراجعة الالكترونية -	0.364	0.097	لا توجد إختلافات جوهرية
4	حماية المعلومات - إجراءات حوكمة تكنولوجيا المعلومات وتفعيل أساسيات الحوكمة الإلكترونية وسياسة أمن المعلومات والشبكات.	0.074	0.304	لا توجد إختلافات جوهرية
5	حماية المعلومات - إجراءات الخاصة بالتعاقد مع شركات الدولية لحماية الاختراقات من داخل المؤسسة والوصول غير المصرح به للبيانات وتعديلها.	0.112	0.375	لا توجد إختلافات جوهرية
	التحليل الاحصائي الكلي للمتغيرات	**0.278**	**0.2198**	**لا توجد إختلافات جوهرية**

ثالثا: الإحصــاء الوصــفي – إدارة المخاطر الخارجية للتحول الرقمي: تبين نتائج التحليلات الإحصــائية الواردة بالجدول (7) أن المتوسط الحسابي الإجمالي للنتائج الإحصائية: يتراوح بين (4.557) للسؤال: " إجراءات إدارة المخاطر – فيما يخص قياس الثغرات في النظام والأنظمة المرتبطة بالمعلومات من خلال إجراءات الهكر التجريبي حسب مؤسسات الدولية ذات الاختصاص "، مما يعني أن الاتجاه العام لإجابات المشاركين "موافقون بشدة" على الأسئلة، و (3.687) للسؤال: " اجراءات أدارة المخاطر – حوكمة تكنولوجيا المعلومات فيما يخص أمن الشبكات والاتصال للحفاظ علي سرية المعلومات وعدم الوصول المرخ من خارج المؤسسة للمعلومات المحاسبية" تبين أنهم يوافقون على أثر إدارة المخاطر الخارجية.

جدول (7) - الاحصاء الوصفي - إدارة مخاطر التحول الرقمي - الخارجية

ر.م	الفقــرات	Mean	dev-Std	Min Max	الموافقة ورفض	قوة تأثير
1	اجراءات إدارة المخاطر – ضد الكوارث الطبيعية من وجود نسخ احتياطي للنظام المعلومات – وأنظمة بديلة للعمل في ظروف القاهرة – وحل المشاكل وتعقيدها من خارج المؤسسة.	4.425	0.875	Max	موافقة بشدة	تأثير قوي جداً
2	اجراءات إدارة المخاطر – حوكمة تكنولوجيا المعلومات فيما يخص أمن الشبكات والاتصال للحفاظ علي سرية	3.687	0.759	Max	موافقة	مؤثر

	المعلومات وعدم الوصول المرخص من خارج المؤسسة للمعلومات المحاسبية.					
3	إجراءات إدارة المخاطر – فيما يخص التطبيقات الذكية في شبكات الدولية للأنترنت سواء كانت علي هواتف المحولة أو أجهزة حاسوب وإجراءات الرقابة والخصوصية العالية لها وكذلك اعتماد برامج أمان عالية لها.	4.215	0.999	Max	موافقة بشدة	تأثير قوي
4	إجراءات إدارة المخاطر – التقاعد مع شركات دولية كبري فيما يخص حماية المعلومات والوصول غير المصرح للبيانات واعطاء الانذار والتنبيهات في حاله محاولة الوصول غير المصرح به.	3.995	1.012	Max	موافقة	مؤثر
5	إجراءات إدارة المخاطر – التحديث الدوري للنظام وتطويره يساهم في حماية المعلومات من العبث والوصول غير المصرح به.	4.088	0.768	Max	موافقة بشدة	تأثير قوي جداً
6	إجراءات إدارة المخاطر – فيما يخص قياس الثغرات في النظام والأنظمة المرتبطة بالمعلومات المحاسبية من خلال إجراءات الهكر التجريبي حسب مؤسسات الدولية ذات الاختصاص.	4.557	0.759	Max	موافقة بشدة	تأثير قوي جداً
7	الإجراءات الخاصة بالتعامل مع أطراف خارج المؤسسة مثل المراجعين الخارجيين وسمتعهم والشركات التي تقدم خدمات تقنية وتتطلع علي البيانات الخاصة بالمؤسسة وتتعامل مع النظام.	3.769	0.999	Max	موافقة بشدة	مؤثر
التحليل الاحصائي الكلي للمتغيرات		3.987	0.883	Max	موافقة	مؤثر

رابعا: الإحصـــاء الاســـتدلالي (الاســـتنتاجي) إدارة المخاطر الخارجية للتحول الرقمي: تم أجراء اختبار تحليل التباين الأحادي (One- Way ANOVA) واختبار One Way Kruskal-Wallis من خلال عرض قيم كل سؤال على حده كما هو موضـح بالجدول (8) بينت النتائج أن قيمة (P- Value) أكبر من مسـتوى الدلالة المعنوية 5% في اغلب الأسـئلة، مما يعني عدم وجود فروق ذات دلالة إحصـائية فيما بين متوسطات المجموعات لكل سؤال من هذه الأسئلة، اما باقي الأسئلة بينت النتائج أن قيمة (P- Value)أقل من مســتوى الدلالة المعنوية 5%، كما هو موضــح بالجدول رقم (8) الاختلافات بين اجابات الشــركات بسبب متغير (الخبرة) والتأهيل العلمي.

جدول (8) - الاحصاء الاستنتاجي – إدارة مخاطر التحول الرقمي - الخارجية

ر.م	الفقــرات	One– Way Anova	One-Way K.W	MCT
1	اجراءات إدارة المخاطر – ضد الكوارث الطبيعية من وجود نسخ احتياطي لنظام المعلومات – وأنظمة بديلة للعمل في ظروف القاهرة – وحل المشاكل وتعقيدها من خارج المؤسسة.	0.348	0.208	لا توجد إختلافات جوهرية
2	اجراءات إدارة المخاطر – حوكمة تكنولوجيا المعلومات فيما يخص أمن الشبكات والاتصال للحفاظ علي سرية المعلومات وعدم الوصول المرخص من خارج المؤسسة للمعلومات المحاسبية.	0.471	0.014	توجد إختلافات جوهرية

3	إجراءات إدارة المخاطر – فيما يخص التطبيقات الذكية في شبكات الدولية للأنترنت سواء كانت على هواتف المحولة أو أجهزة حاسوب وإجراءات الرقابة والخصوصية العالية لها وكذلك اعتماد برامج أمان عالية لها.	0.364	0.097	لا توجد إختلافات جوهرية
4	إجراءات إدارة المخاطر – التعاقد مع شركات دولية كبري فيما يخص حماية المعلومات والوصول غير المصرح للبيانات واعطاء الانذار والتنبيهات في حاله محاولة الوصول غير المصرح به.	0.074	0.304	لا توجد إختلافات جوهرية
5	إجراءات إدارة المخاطر – التحديث الدوري للنظام وتطويره يساهم في حماية المعلومات من العبث والوصول غير المصرح به.	0.112	0.375	لا توجد إختلافات جوهرية
6	إجراءات إدارة المخاطر – فيما يخص قياس الثغرات في النظام والأنظمة المرتبطة بالمعلومات من خلال إجراءات الهكر التجريبي حسب مؤسسات الدولية ذات الاختصاص.	0.471	0.014	توجد إختلافات جوهرية
7	الإجراءات الخاصة بالتعامل مع أطراف خارج المؤسسة مثل المراجعين الخارجيين وسمتعهم والشركات التي تقدم خدمات تقنية وتتطلع علي البيانات الخاصة بالمؤسسة وتتعامل مع النظام.	0.364	0.097	لا توجد إختلافات جوهرية
التحليل الاحصائي الكلي للمتغيرات		0.278	0.2198	لا توجد إختلافات جوهرية

- **اختبار الفرضية الرئيسية للدراسة:**

تم استخدام اختبار (T –Test) One Sample لاختبار فرضيات الدراسة، حيث تم صياغة الفرضيات الرئيسية بشكل إحصائي (المتوسط النظري ≤ M :H1)، ويتم احتساب قيمة المتوسط النظري لكل فرضية رئيسية على أساس قيمة المتوسط النظري (3)، قبول ورفض الفرضية يتم بناءً على تحديد كل من قيمة (P – Value)، حيث يتم قبول الفرضية إذا كانت قيمة (P – Value) أقل من مستوى الدلالة المعنوية 5 % أو تساويها والعكس في حالة الرفض.

جدول (6) اختبار T-Test للكشف عن تأثير إدارة مخاطر التحول الرقمي

المشاركين (عينة الدراسة)	المتوسط المرجح	الانحراف المعياري	فرق بين المتوسطين	قيمة T	(P V)
126	4.118	0.940	1.118	23.166	0.000

" تؤثر إدارة مخاطر التحول الرقمي تأثيراً جوهري في تحسين كفاءة أمن المعلومات " تبين نتائج اختبار (T-Test) الواردة بالجدول (6) لكل مجموعة على حده ولجميع المجموعات، أن قيمة (P V) لجميع الأسئلة الخاصة بهذه الفرضية أقل من مستوى الدلالة المعنوية 5 %، وعليه تم قبول الفرضية الرئيسية الأولي للدراسة. وتبين نتائج اختبار الفرضيات الفرعية الموجودة في الجدول (7).

جدول (7) اختبار T-Test للفرضيات الفرعية للكشف عن تأثير إدارة المخاطر الداخلية والخارجية

م	الفرضية الفرعية	قيمة الإحصاء (t)	درجة الحرية d.f	الدلالة الاحصائية P_value	النتيجة
1	تؤثر إدارة مخاطر الداخلية للنظم تأثيراً جوهريا موجبا في تحسين جودة المعلومات.	406.24	125	.000	قبول الفرضية
2	تؤثر إدارة مخاطر الخارجية للنظم تأثيراً جوهريا موجبا في تحسين جودة المعلومات.	202.25	125	.000	قبول الفرضية

النتائج والخاتمة:

شهدت تكنولوجيا المعلومات تطورات متلاحقة في الأنظمة الالكترونية وانتقالها من العمل اليدوي الي العمل الالكتروني، اصبحت أكثر مخاطرة واقل اماناً من الأنظمة التقليدية (اليدوية)، ونظراً لاعتماد أنظمة المعلومات حالياً على البيئة الالكترونية (تكنولوجيا المعلومات الرقمية)، وحفظ بياناتها على ملفات الكترونية يستطيع عدد كبير من الأشخاص الوصول إليها. وأن استخدام المصارف إلى تكنولوجيا المعلومات والتحول الرقمي بشكل مواكب لمتطلبات سوق العمل التنافسي في القطاع، أدي لوجود مسؤوليات جديدة فُرضت على المصارف الليبية بذل المزيد من الجهود لتفادي المخاطر التحول الرقمي، ويمكن استخلاص أهم النتائج التي توصلت لها الدراسة فيما يلي:

1. إدارة المخاطر الداخلية وحماية أمن المعلومات في ظل التحول الرقمي وتكنولوجيا المعلومات تشكل أهمية بالغة، مقارنة بالمخاطر الخارجية، وحسب ما توصلت لها عدد من الدراسات غالبا ما تحدث المخاطر الخارجية بأسباب لها علاقة بداخل المؤسسة أو طرف منها.
2. تشكل الجوانب الرقابية للهيكل التنظيمي بالمؤسسات وتحديد الصلاحيات والمسؤوليات والإجراءات التنظيمية الرقابية عامل هام في حماية أمن المعلومات.
3. تساهم حماية الأجهزة والأرقام السرية المشفرة وعدم تدويرها وأنظمة المراقبة الداخلية مثل: كاميرات المراقبة وبرامج الحماية والمراجعة الالكترونية الدورية والطارئة أحد أهم العوامل التي تعمل لحماية البيانات والمعلومات وتفعل أمن المعلومات بشكل كفوء.
4. تساهم إجراءات حوكمة تكنولوجيا المعلومات وتفعيل أساسيات الحوكمة الإلكترونية وسياسة أمن المعلومات والشبكات داخل وخارج المؤسسات في حماية آمن المعلومات.
5. وجود نسخ احتياطي لنظم المعلومات وأنظمة بديلة للعمل في الظروف القاهرة وحل المشاكل وتعقيدها من خارج المؤسسة تساهم في حماية أنظمة المعلومات ضد الكوارث الطبيعية.
6. التحديث الدوري للنظام وتطويره يساهم في حماية المعلومات من العبث والوصول غير المصرح به.
7. تساهم الإجراءات الرقابية وشروط التعاقد الخاصة بسرية البيانات مع أطراف خارج المؤسسة مثل المراجعين الخارجيين والشركات التي تقدم خدمات تقنية في تعزيز آمن المعلومات.

التوصيات:

1. يجب الاهتمام بالتأهيل العلمي والعملي للعاملين بإدارات المحاسبة والمخاطر في المصارف التجارية في مجال أمن المعلومات، وذلك لمواجهه المخاطر التقنية الناتجة من التطور التكنولوجي والرقمي.
2. يجب إعداد الخطط والاستراتيجيات اللازمة التي تعمل على مواجهة أي مخاطر محتملة من التطورات التقنية والتطبيقات الذكية التي يعمل بها القطاع المصرفي في ليبيا.
3. توصي الدراسة بأهمية إعداد سياسات واستراتيجيات من قبل مجلس الإدارة لحماية أمن المعلومات ضد أي تهديدات تصيب النظام وإلزام الإدارة بها ومتابعة لجنة المراجعة والمراجعة الداخلية في اعداد تقارير دورية عن أي اختراقات لنظام المعلومات.
4. إعداد ميثاق شرف للعاملين بالقطاع المصرفي لتعرضه للعديد من المخاطر، واختيار الموظفين والمسؤولين بناءً على النزاهة والأخلاقيات الوظيفية.
5. توصي الدراسة بإعداد دليل للحماية الفنية لنظام المعلومات واعداد برامج الفيروسات والحماية واتخاذ إجراءات النسخ الاحتياطي بشكل دائم ومستمر، مع الاحتفاظ بنظام احتياطي للعمل في حال تعرض النظام الرئيسي لأي مخاطر.
6. الالتزام بالمعايير الدولية، وعدم الإفصاح عن معلومات غير مصرح بها وإعداد السياسات اللازمة لحماية التقارير والمعلومات السرية.
7. يجب الإفصاح عن المخاطر والتهديدات المحتملة والخسائر التي قد تحققها المصارف الليبية نتيجة الاختراقات والتهديدات التي تصيب أمن معلوماتها.
8. يجب على مصرف ليبيا المركزي إعداد خطط ودليل عملي وعلمي لتطبيق استراتيجية أمن المعلومات والاتجاه نحو استراتيجيات حديثة مثل الأمن السيبراني.

أفاق الدراسات المستقبلية:

إن موضوع الدراسة الحالية والخاص بدور إدارة مخاطر التحول الرقمي في تحسين كفاءة أمن المعلومات، أبرز النتائج المتحصل عليها النظرية والعملية، وتوصيات الدراسة، فانة بالإمكان اقتراح إجراء الدراسات التالية:

1. دراسة تأثير التحول الرقمي ومهنة المحاسبة والمراجعة.
2. دراسة الأمن السيبراني في الحد من مخاطر التحول الرقمي.
3. حوكمة تكنولوجيا المعلومات وأثرها على التطور الرقمي.

قائمة المراجع

1. العنزي، سالم محمد (2020)، " دور التحول الرقمي في تفعيل آليات ضبط مخاطر التكنولوجيا المالية وأثرها على الخدمات المصرفية الإلكترونية في ظل أزمة كوفيد 19" دراسة ميدانية على البنوك الكويتية – مجلة العلمية للدراسات والبحوث المالية والإدارية.
2. علي، أسامه عبدالسلام، (2011)، " التحول الرقمي للجامعات المصرية" المتطلبات والآليات" المجلس العالمي لجامعيات التربية المقارنة – الجمعية المصرية للتربية المقارنة والإدارة التعلمية، مجلد 14، عدد 33، ص 270.
3. العرود، شاهر والختانة، وحيد والشرفاء، أمجد، (2011)، " تأثير تطبيق مدققي الحسابات لأساليب تكنولوجيا المعلومات على إتمام عملية التدقيق الإلكترونية في الاردن"، مجلة المحاسبة والإدارة والتأمين، جامعة القاهرة، العدد رقم (78)، ص 1-28.
4. عبد الرازق، سحر مصطفى، (2019)، " التحول الرقمي تحدي جديد لمهنة المحاسبة والمراجعة لدعم التنمية المستدامة"، المؤتمر السنوي الرابع والعشرون لبحوث والازمات بعنوان " إدارة التحول الرقمي لتطبيق رؤية مصر 2030 جامعة عين شمس.

5. شاكير، ندي عبد القيوم، (2020)، "واقع نظم المعلومات المحاسبية في القطاع المصرفي في ليبيا- دراسة ميدانية"، كلية الاقتصاد، قسم المحاسبة، الأكاديمية الليبية، رسالة ماجستير غير منشورة.
6. كمال، جودة أحمد، (2021)، "تأثير إدارة مخاطر المالية على تكنولوجيا المعلومات: دراسة وصفية"، رسالة ماجستير غير منشورة، كلية التجارة، جامعة عين شمس.
7. اكريم، حمزة محمد، (2021)، "دور آليات الحوكمة في الحد من مخاطر نظم المعلومات المحاسبية – المصارف الليبية"، رسالة دكتوراه غير منشورة، كلية العلوم الاقتصادية والتصرف، جامعة صفاقس.
8. البسيوني، بسمة عبد الرحمن، (2021)،" دور أثر الحوسبة السحابية كأحد تقنيات التحول الرقمي علي هيكل التكاليف"، المجلة البحوث المالية للتجارية والتمويل، كلية التجارة، جامعة بور سعيد، العدد (2)، المجلد (2)، ص ص 652- 667.
9. تقارير ديوان المحاسبة الليبي، (2016-2020)، مطبوعات والنشر، المؤسسة الليبية /https://audit.gov.ly.
10. الجرد، عبد الرحمن الطاهر، (2020)، "تقييم دور نظم المعلومات المحاسبية من المخاطر المصرفية في ضوء معايير بازل"، مجلة القرطاس للعلوم الانسانية والتطبيقية، العدد (8) مايو، ص ص:385-408 .
11. جلول، محمد البشير، (2016) "دور المراجعة الخارجية في تحسين جودة المراجعة القوائم المالية" دراسة حالة على مؤسسة سونلغاز، رسالة الماجستير كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير- جامعة العربي بن مهدي.
12. جمعة، أحمد، وآخرون (2003) " نظم المعلومات المحاسبية" الأردن، الطبعة الاولى، دار المناهج للنشر والتوزيع.
13. حسن، وسام نعمه، (2011) " مدى مساهمة المدقق الداخلي في تعزيز شفافية المعلومات المحاسبية في ظل معايير المحاسبة الدولية " مجلة تكريت للعلوم الإدارية والاقتصادية المجلد -7، العدد- 22.
14. رشوان، عبد الرحمن محمد سليمان وقاسم، زين عبدالحفيظ أحمد (2020)، "دور التحول الرقمي في رفع كفاءة أداء البنوك وجذب الاستثمارات " المؤتمر الدولي الأول في تكنولوجيا المعلومات والأعمال.
15. أمين، بن سعيد، وعبدالرحيم، نادية ومخلوف، أحمد، (2019)، "مستقبل نظم المعلومات المحاسبية في ظل تكنولوجيا الحوسبة السحابية، بحث مقدم إلى المؤتمر الدولي الثالث " المنظمات الذكية بوابة الانتقال إلى العالمية والأستدامة في العصر الرقمي"، كلية المال والأعمال، جامعة العلوم الإسلامية العالمية، المنعقدة خلال الفترة من 20-21 تشرين ثاني /2019، عمان- الاردن.
16. خميس، آسر أحمد، (2021) " أثر التحول الرقمي على الأداء الوظيفي للعاملين في البنوك التجارية المصرية"، المجلة العلمية للدراسات المالية والتجارية، جامعة دمياط، المجلد 2، العدد 2، ص ص 977-1044.
17. سلايمي، جميلة، وبوشي، يوسف، (2019)،" التحول الرقمي بين الضرورة والمخاطر"، مجلة العلوم القانونية والسياسية، مجلد 10، عدد2، ص 944-967.

18. Al Hanini, E. (2012), The Risks of Using Computerized Accounting Information Systems in the Jordanian Banks; their reasons and ways of Prevention. European Journal of Business and Management, 4(20), 53-63.J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.
19. Bodnar, Jeorge H and William S. Hopwood (1995), Accounting Information System,Englewood Cliffs, N. J. Prentice-Hall 1995.
20. Chinudzi gladmore , takudzwa c. maradze & thabani nyoni (2020) " the impact of digital banking on the performance of commercial
21. Chinudzi gladmore , takudzwa c. maradze & thabani nyoni (2020), the impact of digital banking on the performance of commercial banks. Zimbabwe www.jiarjie.com
22. Inaam M. Al-Zwyalif, (2020), IT Governance and its Impact on the Usefulness of Accounting Information Reported in Financial Statements", International Journal of Business and Social Science, Vol. 4, No. 2, PP.83-93.
23. International Auditing and Assurance Standards Board (IAASB), Non- Authoritative Support Material Related to Technology: Audit Documentation when Using Automated Tools and Techniques, April 2021.

24. Ismail, N. & King, M. (2007), Factors influencing the alignment of accounting information system in system in small and medium sized Malaysian manufacturing firms, Vol.1. Issue, ½: 2007, P.15.
25. Kamala Raghavan, (2021), "Impact of Pandemic and Digital Transformation on Global Accounting Profession" journal of Global Awareness Volume 2 Number 1 Article 7 May 2021: https://scholar.stjohns.edu/jga/vol2/iss1/ 7.
26. Muhrtala, T. O., & Ogundeji, M. (2013). Computerized Accounting Information Systems and Perceived Security Threats in Developing Economies: The Nigerian Case. Universal Journal of Accounting and Finance, 1(1), 9-18.
27. Nader Rezaei, (2018), The Evaluation of Implementing IT Governance Controls", Journal of Applied Business and finance Researches, Vol. 2, issue 3, PP. 82-88.
28. Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, (1982), Electron spectroscopy studies on magneto-optical media and plastic substrate interface," IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301.
29. Yose, M. & Choga, F. (2016), Usage of Computerised Accounting Information System at Development Fund Organisations: The Case OfZimbabwe. IOSR Journal of Business and Management (IOSR-JBM), 18(2), p.34.408